



EMBEDDED  
LINUX  
CONFERENCE

@



THE LINUX FOUNDATION  
OPEN SOURCE SUMMIT  
EUROPE

# SBOMs: Essential for Embedded too!

Kate Stewart, VP Dependable Embedded Systems

#ossummit @\_kate\_stewart



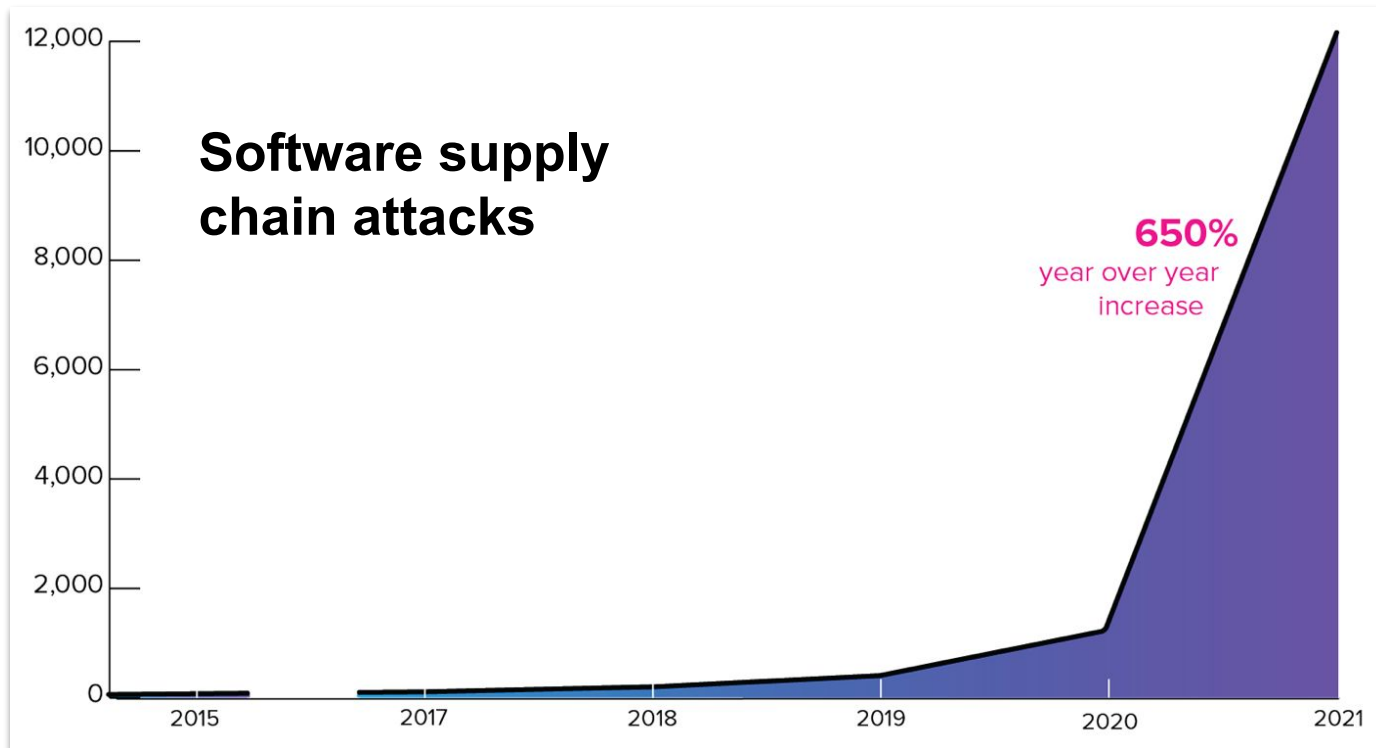
- **Why the interest in SBOMs?**
- What makes up an SBOM?
- How to produce SBOMs for embedded systems?

# Challenge:

Are my products affected by \$vulnerability\$?

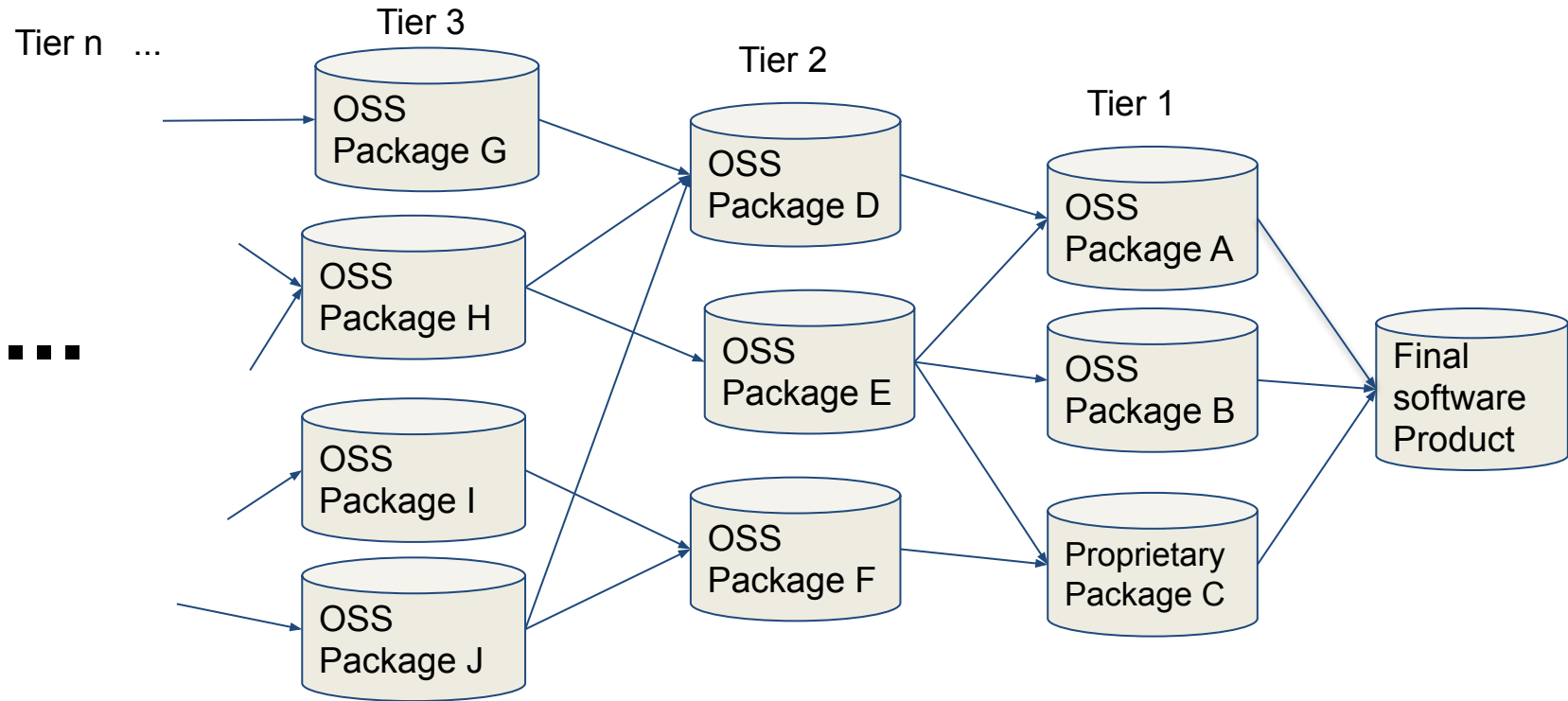


# Software Supply Chain Attacks are Growing...



Sources: Sonatype [2021 State of the Software Supply Chain](#)

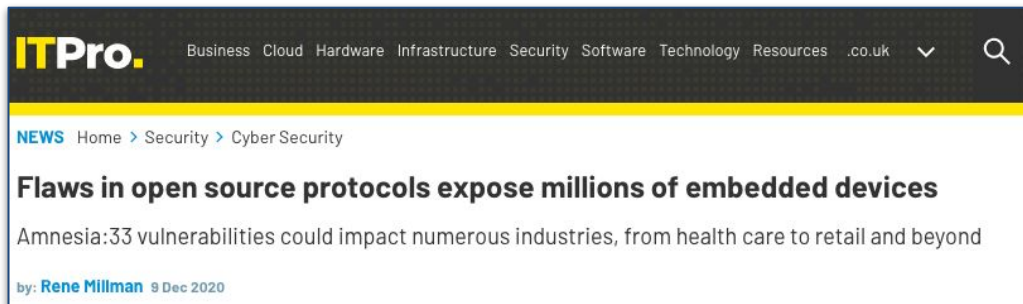
# What is the Software Supply Chain?



Set of **software, suppliers, development processes, and distribution processes** used to **create software products**

# Cost to Remediate?

Cost to developers to fix is small, cost to users....



ITPro. Business Cloud Hardware Infrastructure Security Software Technology Resources .co.uk

NEWS Home > Security > Cyber Security

## Flaws in open source protocols expose millions of embedded devices

Amnesia: 33 vulnerabilities could impact numerous industries, from health care to retail and beyond

by: **Rene Millman** 9 Dec 2020

Source: <https://www.itpro.co.uk/security/cyber-security/358064/flaws-in-open-source-protocols-expose-millions-of-embedded-devices>

## POLICY

# Cleaning up SolarWinds hack may cost as much as \$100 billion

Government agencies, private corporations will spend months and billions of dollars to root out the Russian malicious code

Source: <https://www.rollcall.com/2021/01/11/cleaning-up-solarwinds-hack-may-cost-as-much-as-100-billion/>



FEDERAL TRADE COMMISSION  
PROTECTING AMERICA'S CONSUMERS

## FTC warns companies to remediate Log4j security vulnerability

By: This blog is a collaboration between CTO and DPIP staff and the AI Strategy team | Jan 4, 2022 9:19AM

SHARE THIS PAGE   

TAGS: Accountability | Data security | Patches

Log4j is a ubiquitous piece of software used to record activities in a wide range of systems found in consumer-facing products and services. Recently, a serious vulnerability in the popular Java logging package, Log4j (CVE-2021-44228) was disclosed, posing a severe risk to millions of consumer products to enterprise software and web applications. This vulnerability is being widely exploited by a growing set of attackers.

When vulnerabilities are discovered and exploited, it risks a loss or breach of personal information, financial loss, and other irreversible harms. The duty to take reasonable steps to mitigate known software vulnerabilities implicates laws including, among others, the Federal Trade Commission Act and the Gramm Leach Bliley Act. It is critical that companies and their vendors relying on Log4j act now, in order to reduce the likelihood of harm to consumers, and to avoid FTC legal action. According to the complaint in *Equifax*, a failure to patch a known vulnerability irreversibly exposed the personal information of 147 million consumers. Equifax agreed to pay \$700 million to settle actions by the Federal Trade Commission, the Consumer Financial Protection Bureau, and all fifty states. The FTC intends to use its full legal authority to pursue companies that fail to take reasonable steps to protect consumer data from exposure as a result of Log4j, or similar known vulnerabilities in the future.

Check if you use the Log4j software library by consulting the Cybersecurity and Infrastructure Security Agency (CISA) guidance: <https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance>. If you do use it:

Source: <https://www.ftc.gov/news-events/blogs/techftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability>





Of organizations surveyed,  
**95% are concerned  
about software  
security.**

**SBOM 2021 SURVEY**

Source: <https://www.linuxfoundation.org/tools/the-state-of-software-bill-of-materials-sbom-and-cybersecurity-readiness/>

License: CC-BY-4.0

Of organizations surveyed,  
**98% use open  
source software.**



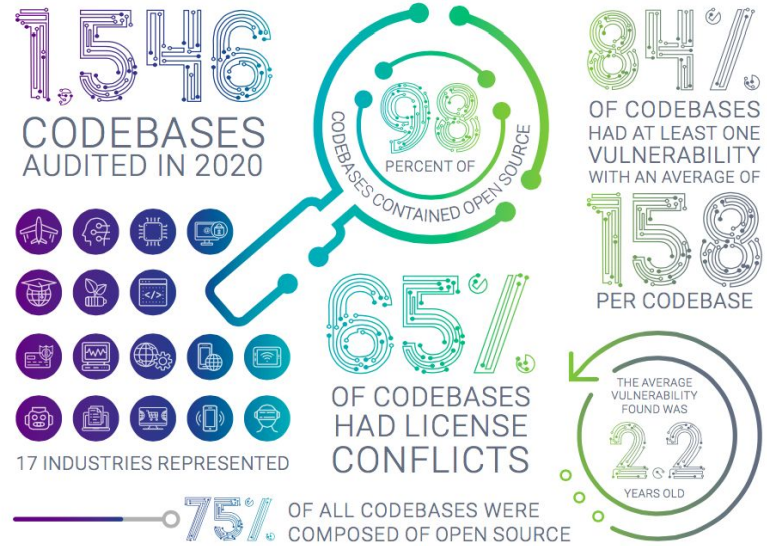
**SBOM 2021 SURVEY**



“98% of codebases audited in 2020 contained open source components.

Open source made up 75% of the audited codebases.”

OVERVIEW



2021 OPEN SOURCE SECURITY AND RISK ANALYSIS REPORT | ©2021 SYNOPSYS, INC.

Source: [2021 Synopsys Open Source Security and Risk Analysis Report](#)

# Transparency is key to improving supply chain security!

## #1 ACTION: **Get a vulnerability reporting system**

in order to better secure your  
software supply chain.



**SBOM 2021 SURVEY**



## #2 ACTION: **Use SBOMS to better secure your software supply chain.**

**SBOM 2021 SURVEY**

Source: <https://www.linuxfoundation.org/tools/the-state-of-software-bill-of-materials-sbom-and-cybersecurity-readiness/>

License: CC-BY-4.0

# Guidelines and Legislation ...

**EUROPEAN UNION AGENCY  
FOR CYBERSECURITY**

**COVID19** | **TOPICS** | **NEWS** | **PUBLIC**

**Find similar publications**

## Guidelines for Securing the Internet of Things


This ENISA study defines guidelines for securing the supply chain for IoT. ENISA with the input of IoT experts created security guidelines for the whole lifespan: from requirements and design, to end use delivery and maintenance, as well as disposal. The study is developed to help IoT manufacturers, developers, integrators and all stakeholders that are involved to the supply chain of IoT to make better security decisions when building, deploying, or assessing IoT technologies.

**Published** November 09, 2020  
**Language** English



**Download**  
PDF document, 1.74 MB

Source: [www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things](https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things)

**CONGRESS.GOV**

Advanced Searches | Browse

Legislation | Examples: hr5, sres9, "health care"

**H.R.1668 - IoT Cybersecurity Improvement Act of 2020**  
116th Congress (2019-2020)

**LAW** | Hide Overview

**Sponsor:** [Rep. Kelly, Robin L. \[D-IL-2\]](#) (Introduced 03/11/2019)  
**Committees:** House - Oversight and Reform; Science, Space, and Technology  
**Committee Meetings:** [06/12/19 10:00AM](#)  
**Committee Reports:** [H. Rept. 116-501](#)  
**Latest Action:** 12/04/2020 Became Public Law No: 116-207. ([TXT](#) | [PDF](#)) ([All Actions](#))

**Tracker:**  
Introduced → Passed House → Passed Senate → To President → **Became Law**

**More on This Bill**  
[Constitutional Authority Statement](#)  
[CBO Cost Estimates \[1\]](#)

**Subject — Policy Area:**  
Government Operations and Politics  
[View subjects >>](#)

Source: <https://www.congress.gov/bill/116th-congress/house-bill/1668/text>

# Regulatory Agencies ...

## CYBERSECURITY NEWS

### Healthcare Sector Spearheads SBOM Adoption to Support Cybersecurity

Healthcare is pioneering SBOM adoption due to growing cybersecurity concerns and the FDA's recent medical device security guidance, the Linux Foundation found.



Source: <https://healthitsecurity.com/news/healthcare-sector-spearheads-sbom-adoption-to-support-cybersecurity>

## 9 rules imposed by NERC CIP standards

- CIP-001** Sabotage reporting
- CIP-002** Critical cyber asset identification
- CIP-003** Security management controls
- CIP-004** Personnel and training
- CIP-005** Electronic security perimeters
- CIP-006** Physical security of critical cyber assets
- CIP-007** Systems security management
- CIP-008** Incident reporting and response planning
- CIP-009** Recovery plans for critical cyber assets

©2022 TECHTARGET. ALL RIGHTS RESERVED.

Source: <https://searchcompliance.techtarget.com/definition/NERC-CIP-critical-infrastructure-protection>



## Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our

- Why the interest in SBOMs?
- **What makes up an SBOM?**
- How to produce SBOMs for Embedded Systems?



# What do SBOM's look like?

## Lots of different forms...

## Need to standardize to automate at scale.



## What third-party software is used by SimpleRisk and how is it licensed?

Modified on: Sat, Mar 14, 2020 at 2:22 PM



Print

As with just about any software product these days, SimpleRisk did not write 100% of the code included in the product. Over the years, we have used a variety of third-party software to provide features and functionality for our user base. In 2019, we performed a full audit of all third-party source code that has been included in the product and verified that we are in compliance with all known licenses for the included software. Below is the Bill of Materials (BOM), produced from that effort, which outlines each of these software packages and the licensing that was found for them. If you are the developer, maintainer, or licensor for any of these packages and believe that this information is in error, we'd ask that you please submit a support ticket to address your concerns.

### SimpleRisk Bill of Materials (BOM)

**SimpleRisk Core:** This is the free and open source offering from SimpleRisk that also forms the basis for both our on-prem and hosted offerings. It is licensed under the Mozilla Public License (MPL) 2.0.

#### PHP Libraries Included in the SimpleRisk Core

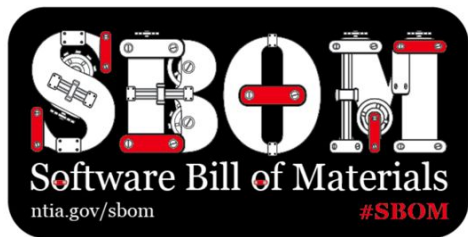
- HighchartsPHP: Licensed under the GNU General Public License (Version 3, 29 June 2007).
- PHPMailer: Licensed under the GNU Lesser General Public License (Version 2.1, February 1999)
- CSRF-Magic (<http://csrf.htmlpurifier.org/>): Licensed under the BSD 2-Clause "Simplified" License.
- Epiphany: Custom copyright notice and license located under `simplerisk/includes/epiphany/LICENSE`.
- Zend Escaper: Custom copyright notice and license located under `simplerisk/includes/Component_ZendEscaper/LICENSE.md`.

#### Javascript Libraries Included in the SimpleRisk Core

- HighCharts: SimpleRisk has purchased a perpetual Highcharts OEM License for unlimited installations. This license applies for all customers using SimpleRisk, regardless of whether they are utilizing it in a hosted or on-premise installation.
- JQuery (<https://jquery.org/>): Licensed under the MIT license.
- JQuery Tree Widget (<https://github.com/daredevel/jquery-tree>): Licensed under the MIT license.
- EasyUI for JQuery ([www.jeasyui.com](http://www.jeasyui.com)): Licensed under the [freeware](#) license.
- Sortable (<https://kryogenix.org/code/browser/sortable/>): Licensed under the X11 license.

Source: <https://simplerisk.freshdesk.com/support/solutions/articles/6000230367-what-third-party-software-is-used-by-simplerisk-and-how-is-it-licensed>

# Software Bill of Materials (SBOM)



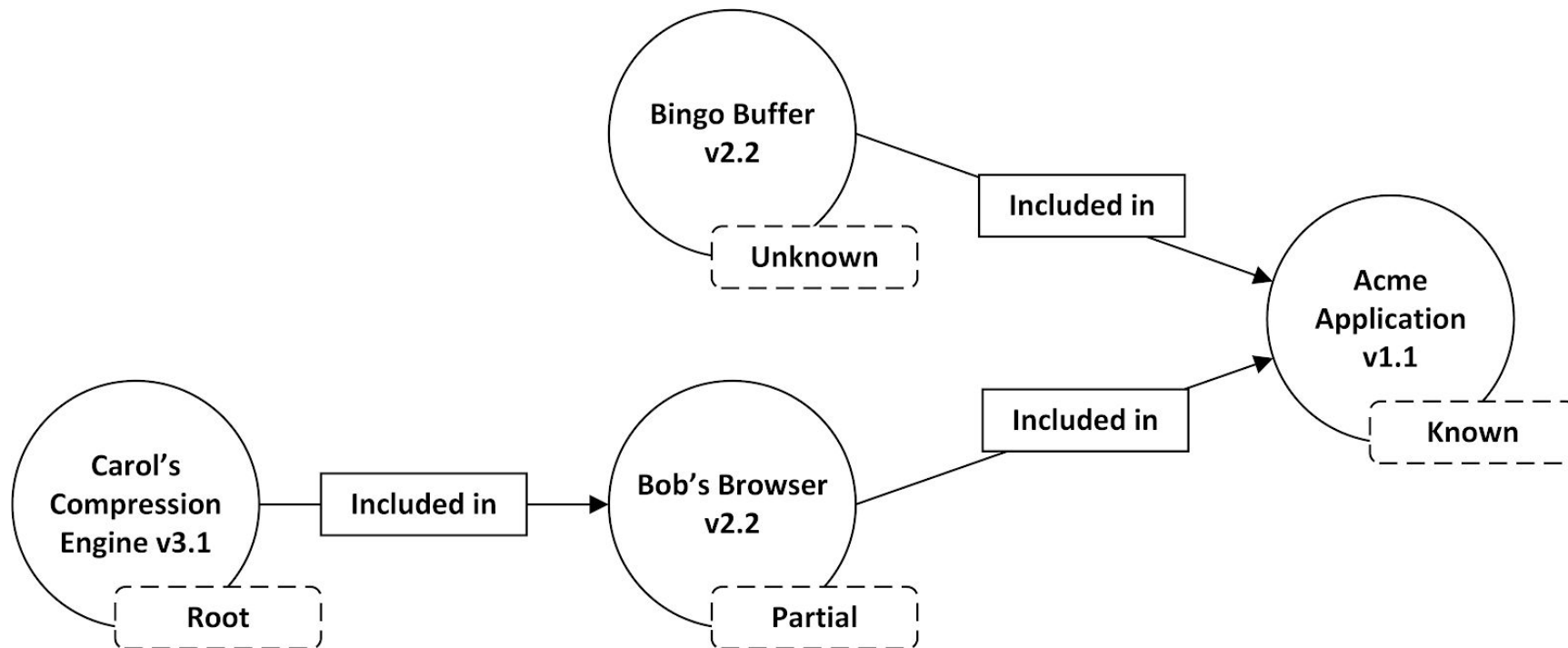
An SBOM is a formal record containing the details and supply chain relationships of various components used in building software.

These components, including libraries and modules, can be open source or proprietary, free or paid, and the data can be widely available or access-restricted.

Source: NTIA's [SBOM FAQ](#)

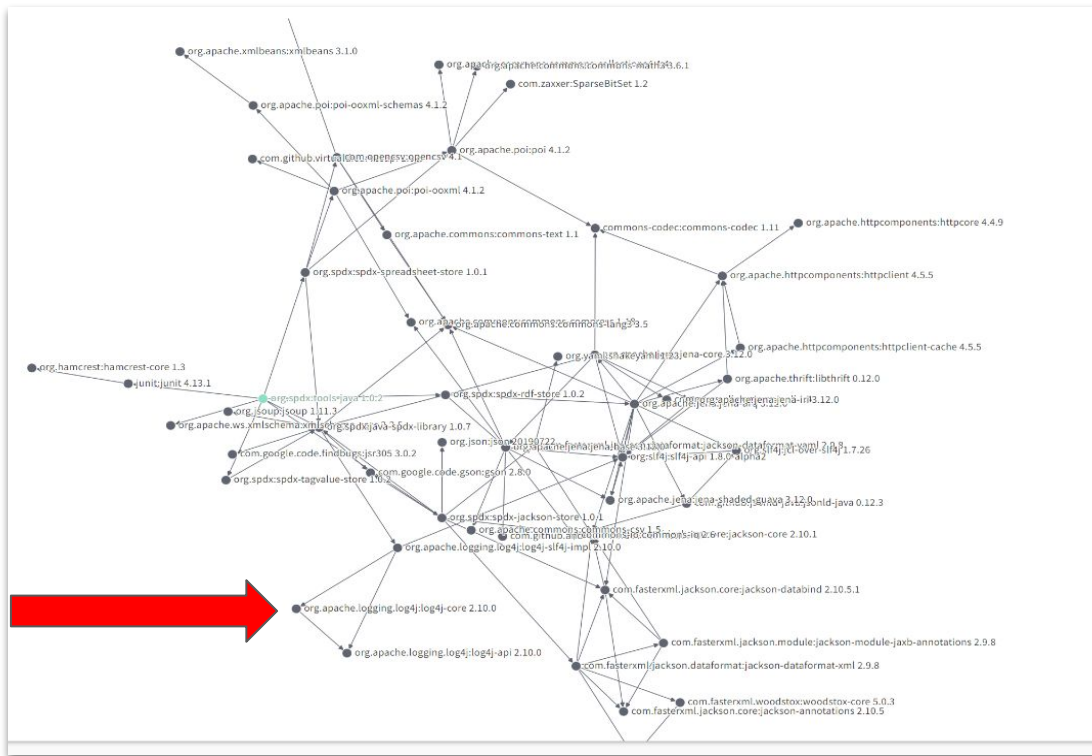


# What does the SBOM represent?



# Challenge: Finding vulnerability in complex software

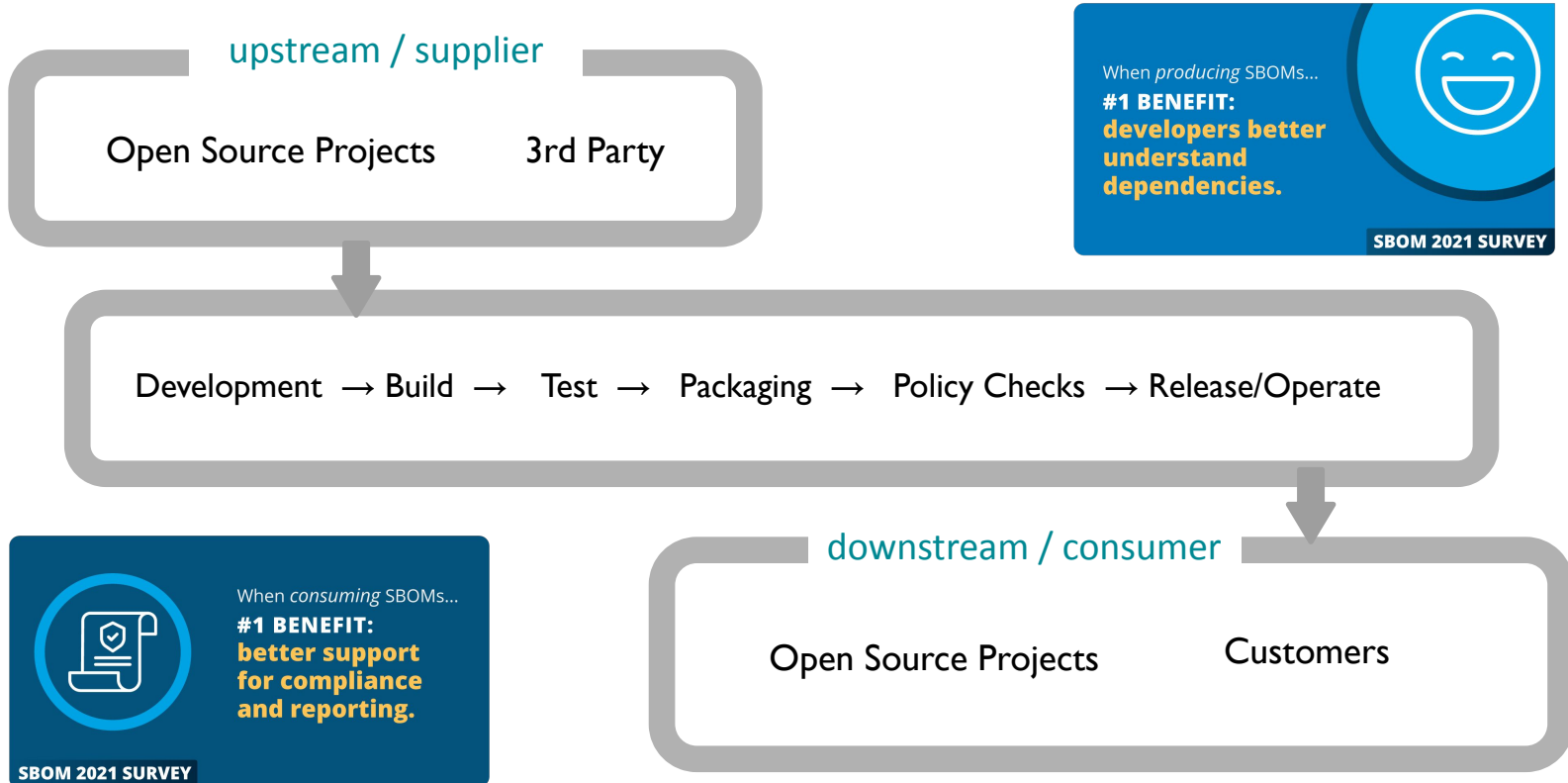
- Need to search the full dependency graph
- Not all dependencies are the same, there are different dependency types (test, build tools, static linked ...)
- No single “UPC code” to clearly identify packages



Source: <https://deps.dev/maven/org.spdx%3Atools-java/1.0.2/dependencies/graph>

License: CC-BY-4.0

# Producing & Consuming SBOMs



# Challenge: Scaling up to the Open Source Ecosystem

open / source / insights

Search for open source packages

All systems

## Remote code injection in Log4j

Overview

Source

GHSA

ID

GHSA-jfh8-c2jp-5v3q

Aliases

CVE-2021-44228

Affected package

[org.apache.logging.log4j:log4j-api](#)  
[org.apache.logging.log4j:log4j-core](#)

Description

# Summary

Summary

36.28k

TOTAL PACKAGES AFFECTED

8.97k

PACKAGES WITH A KNOWN FIX

8.27%

TOTAL ECOSYSTEM AFFECTED

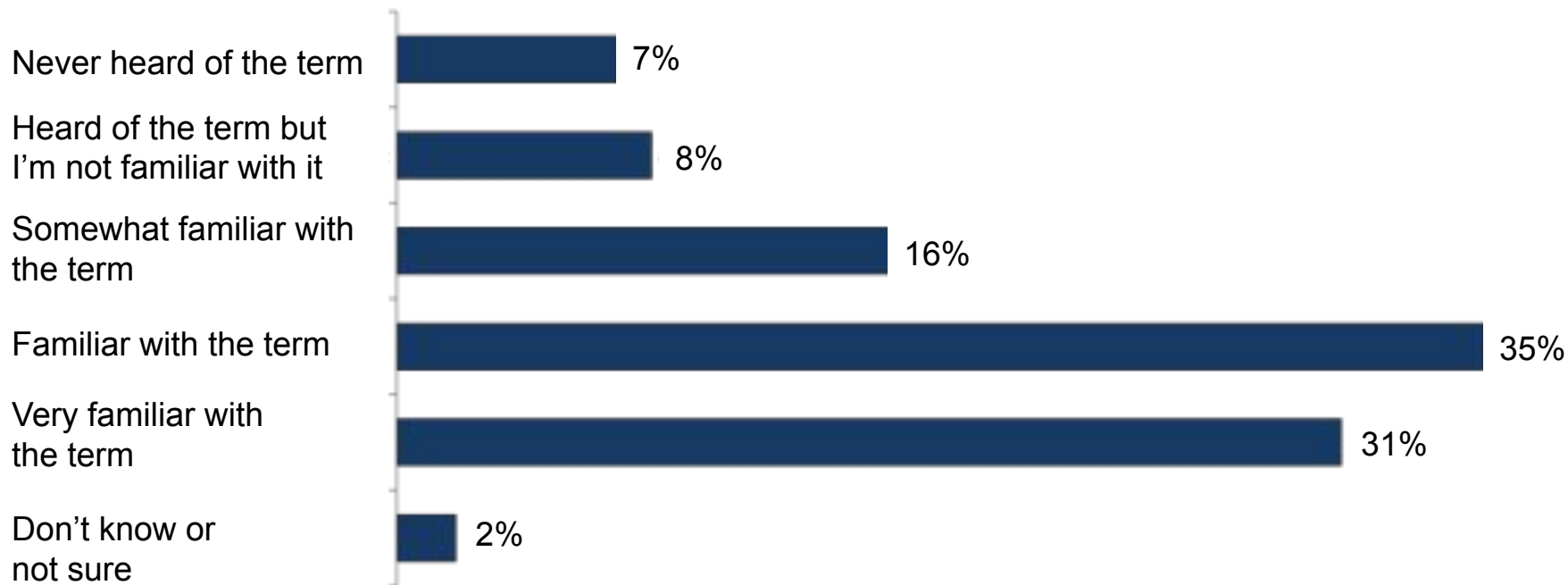
[org.apache.logging.log4j:log4j-api](#)

Affected Version: < 2.15.0

Source: <https://deps.dev/advisory/GHSA/GHSA-jfh8-c2jp-5v3q> on 2022/1/10

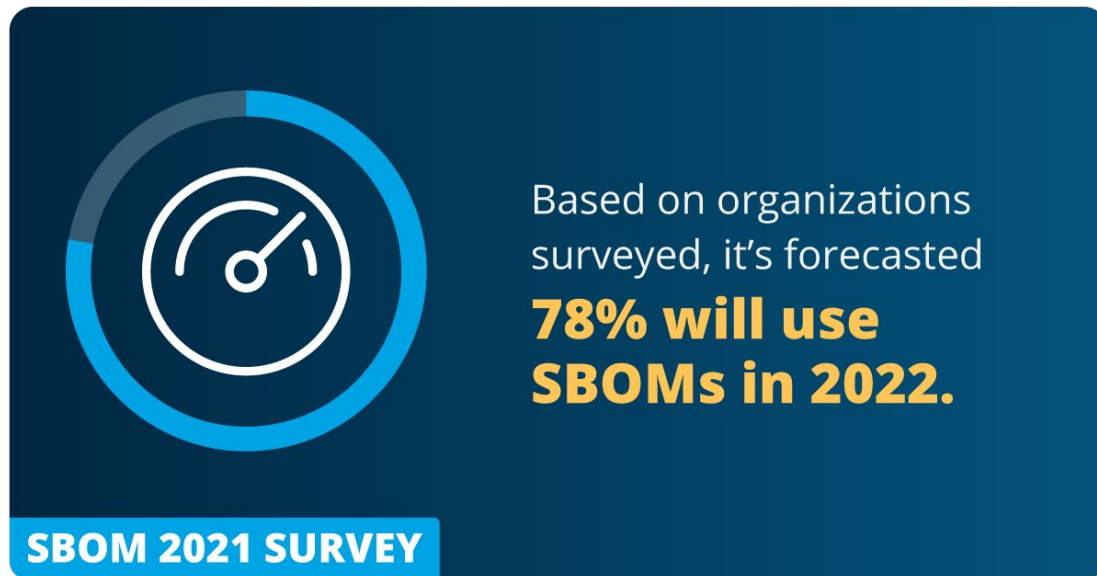
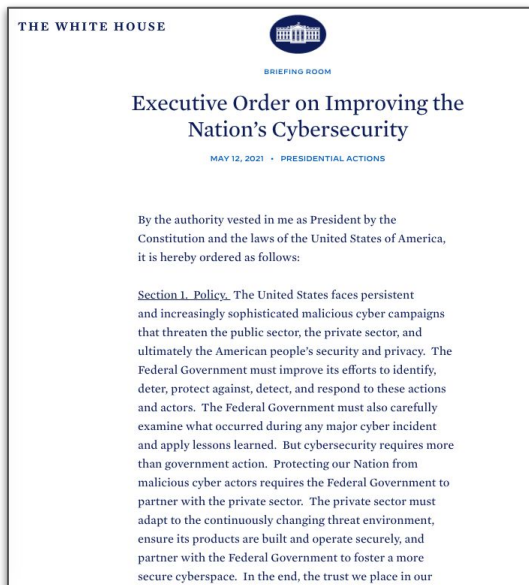
# Industry Awareness of SBOM is emerging...

**What is your organization's familiarity with a software bill of materials (SBOM)?**



Sample Size = 361

# Motivation



Doing this at scale requires standards and tools!

# What is a Minimum SBOM?



## The Minimum Elements For a Software Bill of Materials (SBOM)

Pursuant to  
Executive Order 14028  
on Improving the Nation's Cybersecurity

The United States Department of Commerce

July 12, 2021

Minimum Elements	
<b>Data Fields</b>	Document baseline information about each component that should be tracked: Supplier, Component Name, Version of the Component, Other Unique Identifiers, Dependency Relationship, Author of SBOM Data, and Timestamp.
<b>Automation Support</b>	Support automation, including via automatic generation and machine-readability to allow for scaling across the software ecosystem. Data formats used to generate and consume SBOMs include SPDX, CycloneDX, and SWID tags.
<b>Practices and Processes</b>	Define the operations of SBOM requests, generation and use including: Frequency, Depth, Known Unknowns, Distribution and Delivery, Access Control, and Accommodation of Mistakes.

# What is the Minimum SBOM?

Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Record of the date and time of the SBOM data assembly.

Source: [https://www.ntia.gov/files/ntia/publications/sbom\\_minimum\\_elements\\_report.pdf](https://www.ntia.gov/files/ntia/publications/sbom_minimum_elements_report.pdf).





Of organizations surveyed,  
**47% are using  
SBOMs today.**

**SBOM 2021 SURVEY**

Source: <https://www.linuxfoundation.org/tools/the-state-of-software-bill-of-materials-sbom-and-cybersecurity-readiness/>

License: CC-BY-4.0



Based on organizations surveyed, it's forecasted

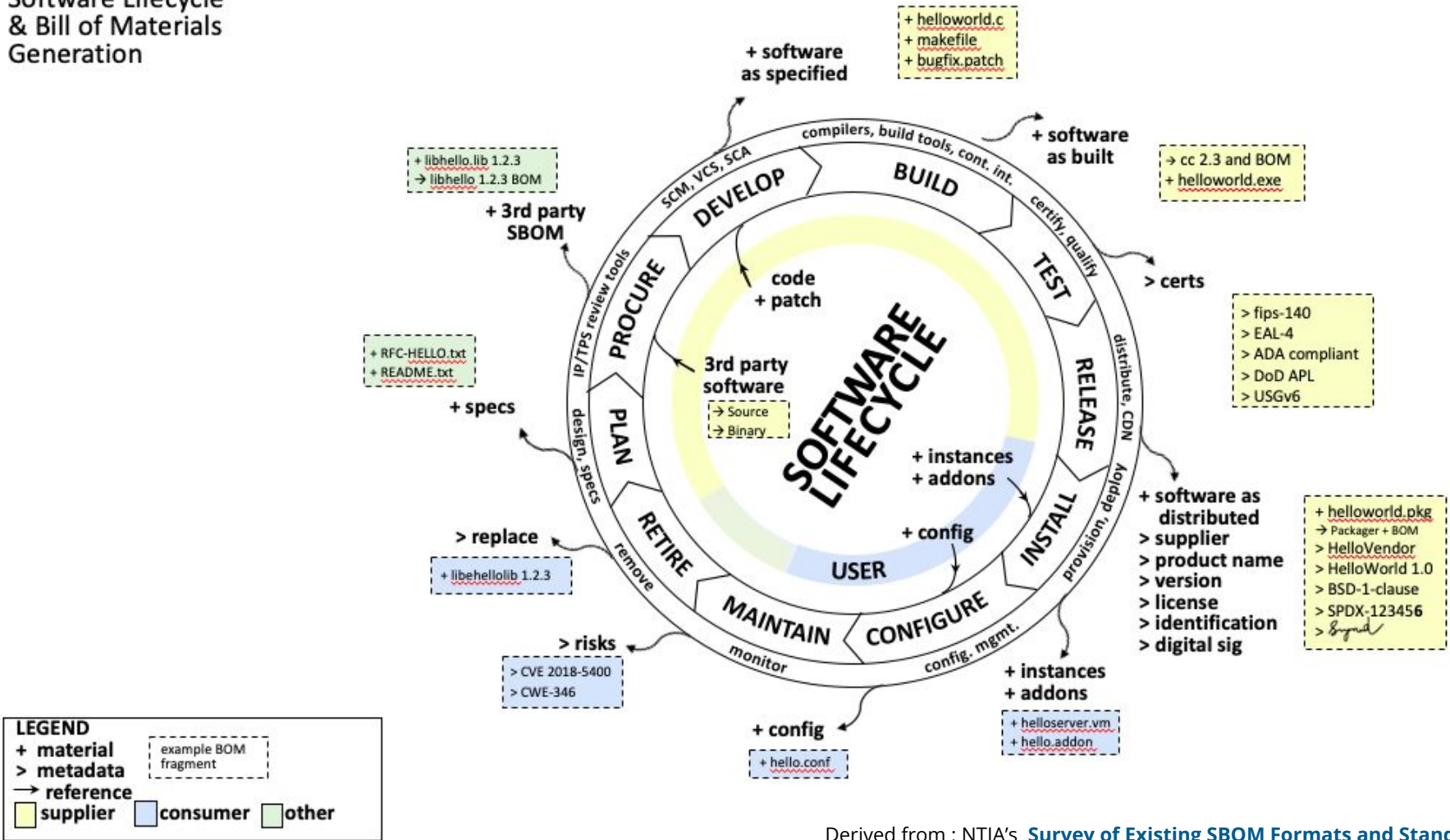
**78% will use SBOMs in 2022.**

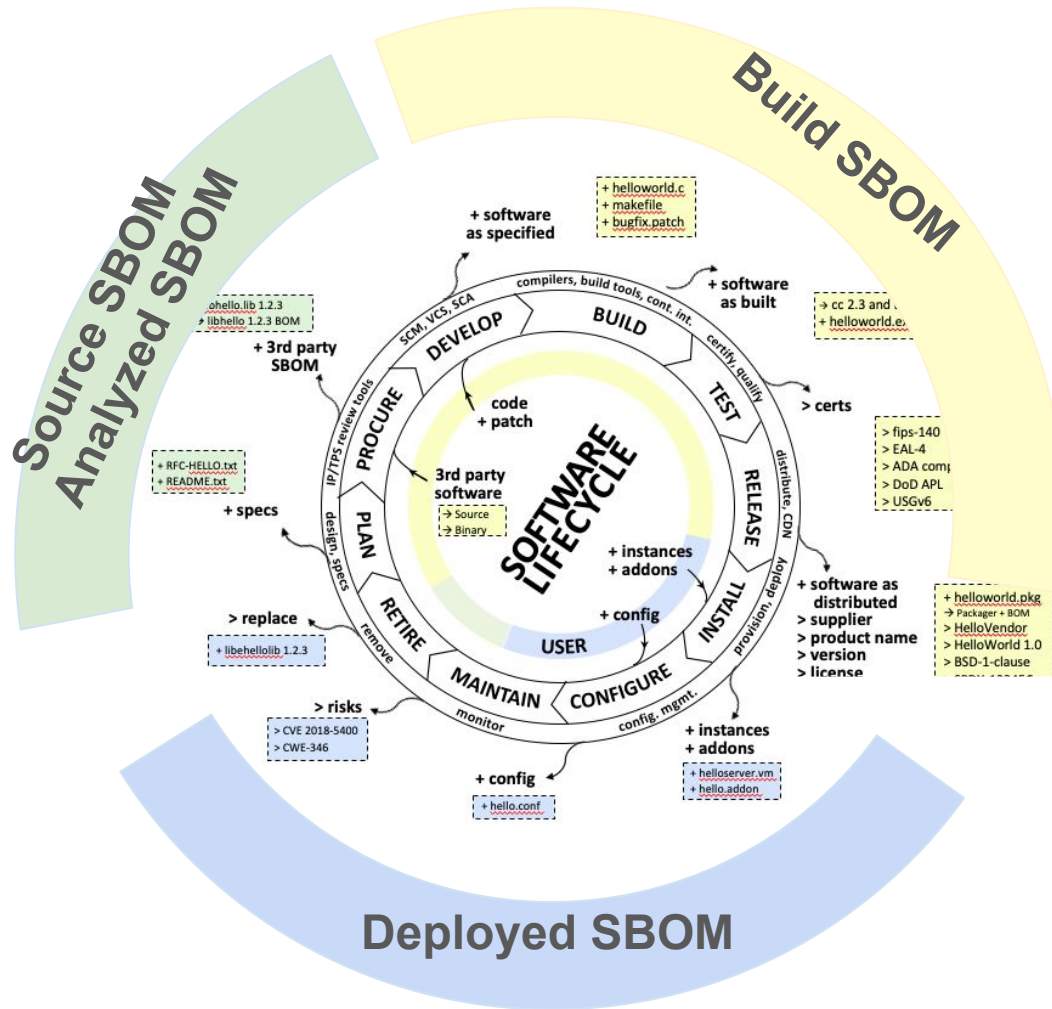
**SBOM 2021 SURVEY**

Source: <https://www.linuxfoundation.org/tools/the-state-of-software-bill-of-materials-sbom-and-cybersecurity-readiness/>

License: CC-BY-4.0

# Software Lifecycle & Bill of Materials Generation





**Source SBOM** - software sources used to build an executable image.

**Analyzed SBOM** - executable image to be integrated into deliverable. Created from 3rd party heuristics.

**Build SBOM** - List of components and relationships between dependent components assembled to create a product released from Supplier.

**Deployed SBOM** - Tracking configuration options on how a product has been deployed by User.

- Why the interest in SBOMs?
- What makes up an SBOM?
- **How to produce SBOMs for embedded systems?**

# Embedded Projects Generating SBOMs



Zephyr's west spdx

Presentation / Demo:

<https://www.youtube.com/watch?v=KYC3YpSu9zs>



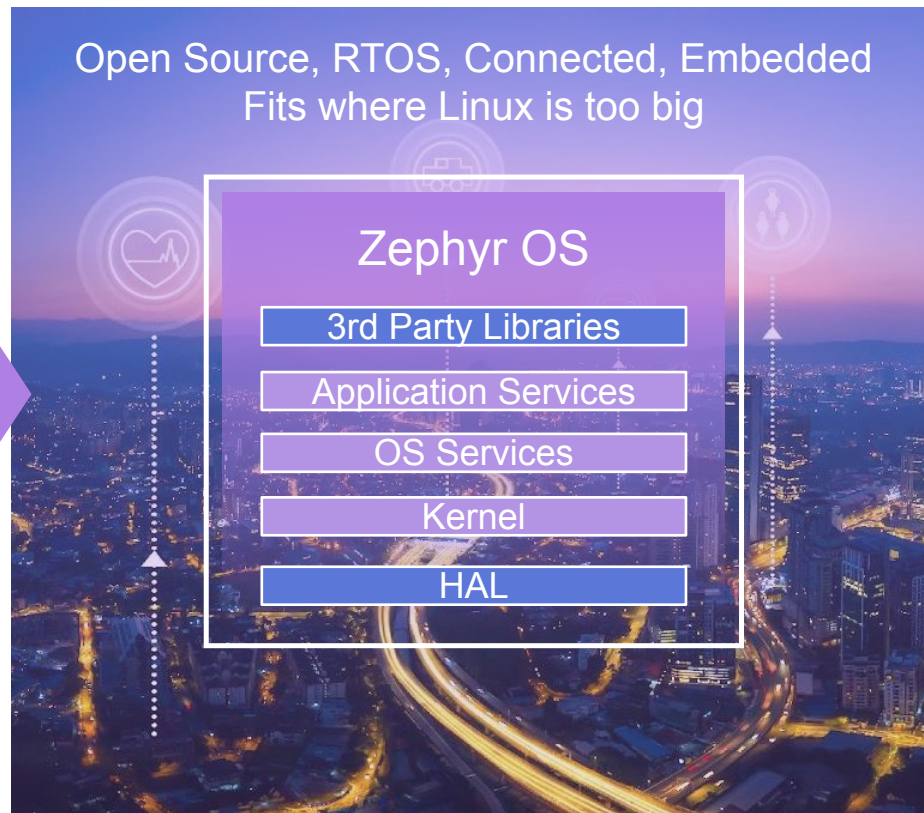
Yocto builds

Presentation / Demo:

<https://www.youtube.com/watch?v=y0N4FnkwTOY>

# Case Study: Zephyr

- **Open source** real time operating system
- **Vibrant Community** participation
- Built with **safety and security** in mind
- **Cross-architecture** with broad SoC and development board support.
- **Vendor Neutral** governance
- **Permissively** licensed - Apache 2.0
- **Complete**, fully integrated, highly configurable, **modular** for **flexibility**
- **Product** development ready using LTS includes security updates
- **Certification** ready with Auditable





# Example of Products Running Zephyr Today



Pro glove



RUUVI Tag



Distancer



Keeb.io BDN9



Hati-ACE



Oticon More



Intellinium Safety Shoes



GNARBOX 2.0 SSD



Anicare Reindeer Tracker



Safety Pod



BLiXT solid state circuit breaker



Moto Watch 100



Point Home Alarm



Rigado IoT Gateway



HereO Core Box



Sentrius



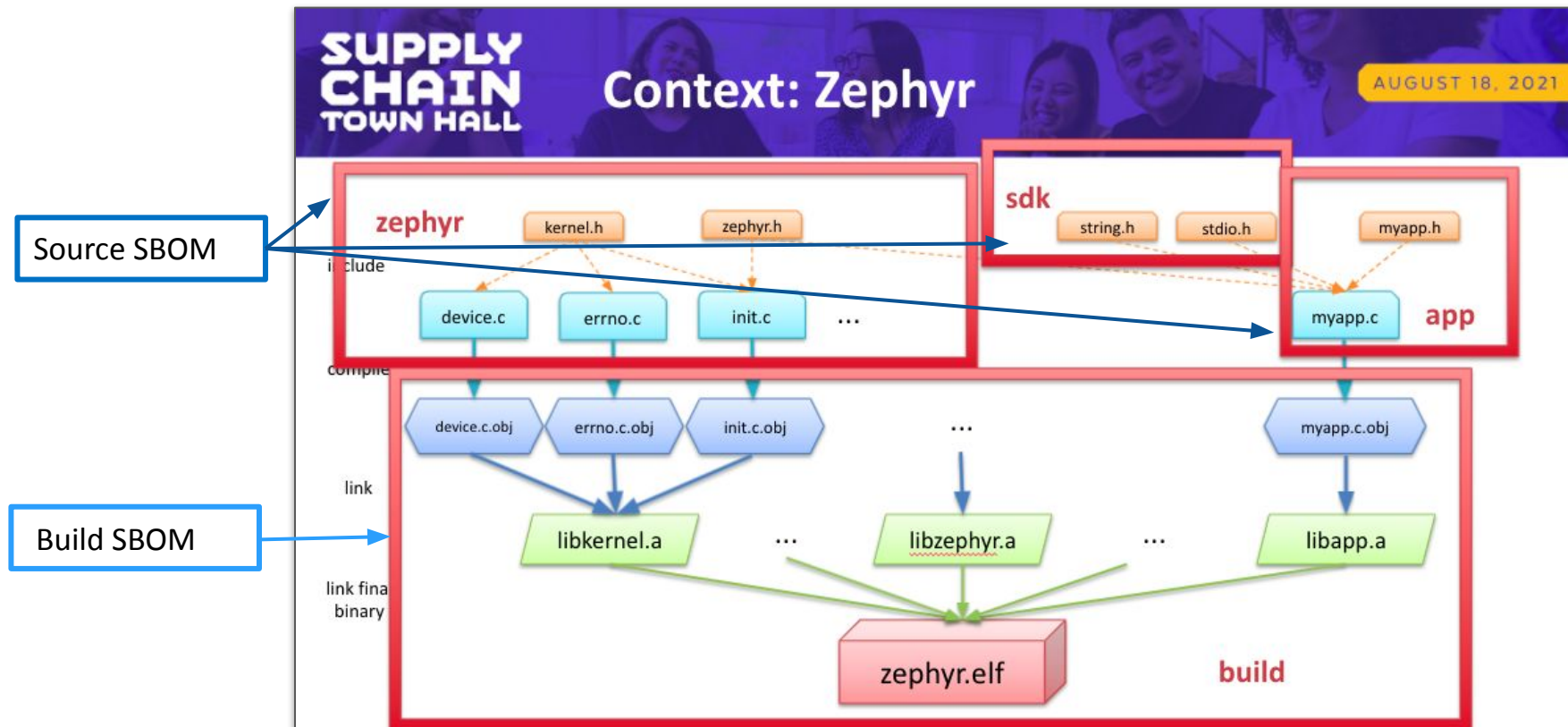
See.Sense AIR



Vestas Wind Turbine



# One Line Config Change to Create SBOMs!



Learn more at: <https://www.youtube.com/watch?v=KYC3YpSu9zs>

# SBOMs Included By Default ... Automatically

64 PASSED

99 PASSED

105 PASSED

115 PASSED

TENSORFLOW

beaglev\_starlight\_jh7100-shell\_module-build.spdx

```

SPDXVersion: SPDX-2.2
DataLicense: CC0-1.0
SPDXID: SPDXRef-DOCUMENT
DocumentName: build
DocumentNamespace: http://spdx.org/spdxdocs/zephyr-f51c77e5-c0b1-4354-b4fe-ce14d141768b/build
Creator: Tool: Zephyr SPDX builder
Created: 2022-01-18T12:43:08Z

ExternalDocumentRef: DocumentRef-app http://spdx.org/spdxdocs/zephyr-f51c77e5-c0b1-4354-b4fe-ce14d141768b/app SHA1: d64b4433e24afbe7c8f02bc6b0224b0ed9dc8e2
ExternalDocumentRef: DocumentRef-zephyr http://spdx.org/spdxdocs/zephyr-f51c77e5-c0b1-4354-b4fe-ce14d141768b/zephyr SHA1: fe54b93ae08866f4774f657aba9608cbd4400a7a

Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-zephyr-final

#### Package: app

PackageName: app
SPDXID: SPDXRef-app
PackageDownloadLocation: NOASSERTION
PackageLicenseConcluded: Apache-2.0
PackageLicenseInfoFromFiles: Apache-2.0
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
FilesAnalyzed: true
PackageVerificationCode: fbf5d511cc04828f9fb7eec86074114eec9b651d

Relationship: SPDXRef-app HAS_PREREQUISITE SPDXRef-syscall-list-h-target
Relationship: SPDXRef-app HAS_PREREQUISITE SPDXRef-driver-validation-h-target
Relationship: SPDXRef-app HAS_PREREQUISITE SPDXRef-kobj-types-h-target
Relationship: SPDXRef-app HAS_PREREQUISITE SPDXRef-zephyr-generated-headers

FileName: ./app/libapp.a
SPDXID: SPDXRef-File-libapp.a
FileChecksum: SHA1: 5e8c866ca73e9c3dda61090d22834b30d484e6e

```

BOARD NAME

ARM (310) ^

ARM64 (8) ^

NIO52 (1) ^

RISCV (17) v

Andes ADP-XC7K AE350

BeagleV Starlight JH7100 (NON-SMP)

ESP32-C3

GigaDevice GD32VF103V-EVAL

SiFive HiFive1

SiFive HiFive1 Rev B

SiFive HiFive Unleashed

SiFive HiFive Unmatched

ut8xxx2\_evb

LiteX SoC with VexRiscv software CPU

Speed Longan Nano

Speed Longan Nano Lite

Microsemi M2GL025 with MIV target

NEORV32 Processor (SoC)

RV32M1-VEGA

STATUS MATRIX

BINARIES ^

ARCHITECTURE v

ARM

ARM64

NIO52

RISCV

X86

XTENSA

BUILD DETAILS

04C47CE0

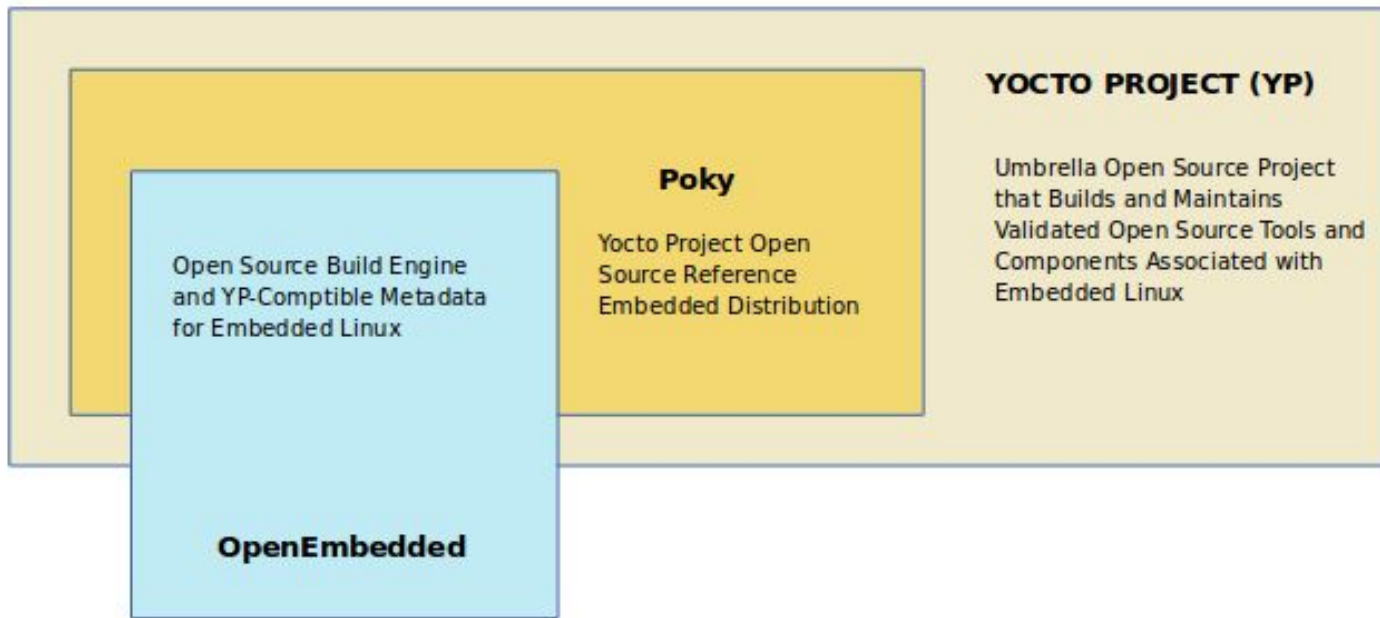
44462723F5

DO YOU WANT YOUR BOARD SUPPORTED IN RENODE?

CONTACT US FOR RENODE SUPPORT SERVICES

Source: <https://www.linux.com/featured/enhancing-supply-chain-security-for-embedded-systems-renod-e-dashboard-for-zephyr-rtos-adds-new-software-bill-of-materials-sbom-capabilities-by-default/>

# Case Study: Yocto & OpenEmbedded



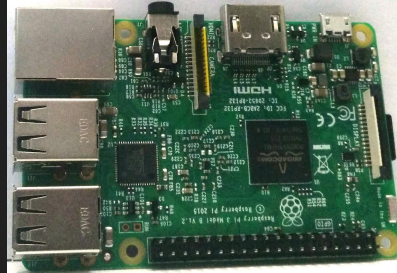
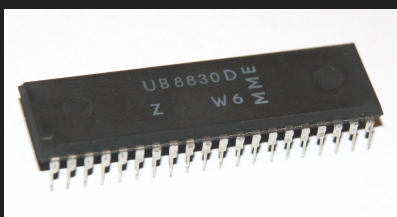
## Yocto Project

- Linux Foundation project
- Poky reference distribution
- Runs QA tests
- Manages release schedule
- Provides funding for personnel
- Documentation

## OpenEmbedded

- Community project
- OpenEmbedded core layer
- Build system (bitbake)

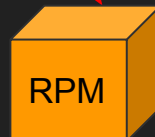
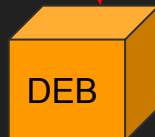
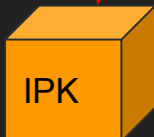
# Images



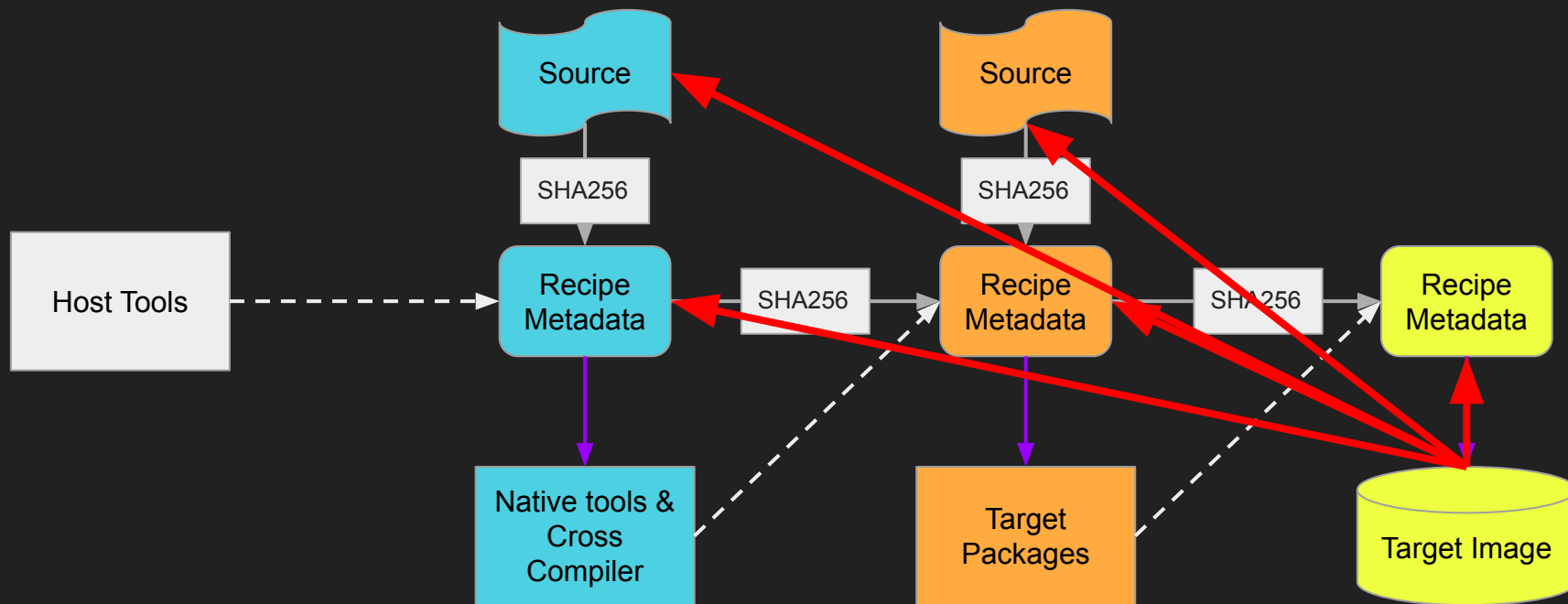
QEMU



Target Image



# Simplified Build Flow



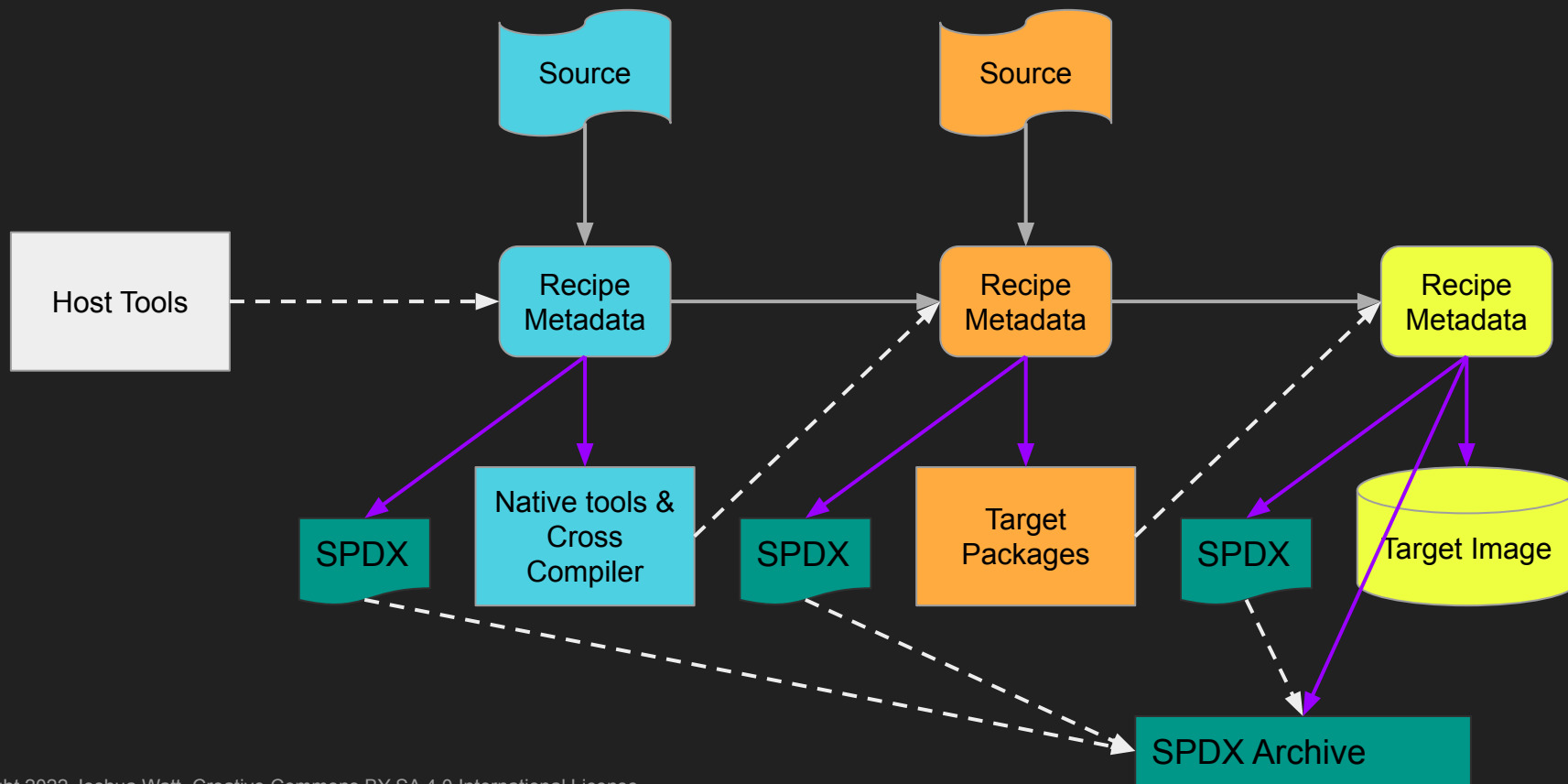
# Recipe Metadata

Recipes already contain much of the data desired in a SBOM

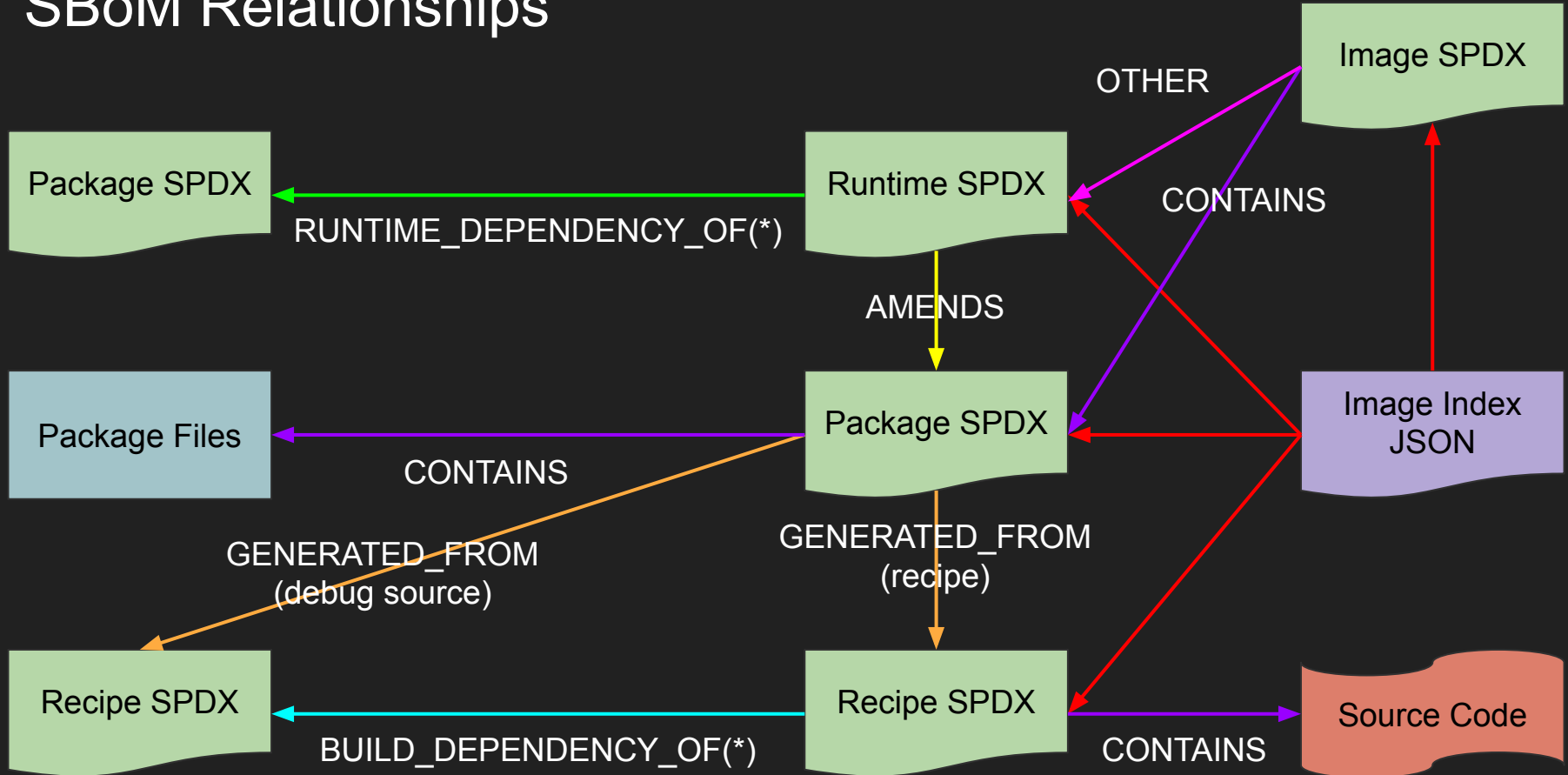
- Version
- Source code URL
- Licenses
- Build time dependencies
- Run time dependencies
- CVEs patched
- Source Files
- Package Files
- ...

**All of this information is authoritative (no guessing)**

# SPDX SBOM Generation with one line config change



# SBoM Relationships





# What can we generate SPDX SBOM documents for?

## TL; DR - Anything we can build

- "On target" C/C++/Fortran etc. ✓
- "Host" build tools ✓
- Linux Kernel ✓
- Target images ✓
- SDKs ✓
- Container Images ✓
- VM Images ✓
- Rust ⚠️
- Go ⚠️

To learn more about Yocto & SBOM generation see:  
<https://www.youtube.com/watch?v=8X5PWa7A6pY>

# Yocto SPDX Features

- Declared License
  - With License Text if not a known SPDX license
- Homepage URL
- Download URL(s)
- CVEs fixed
- CPE
- Summary
- Description
- Source File Listing with Checksums
- Source file SPDX licenses
- Packages
- Package files with Checksums
- Package file GENERATED\_FROM (from debug data)
- Build time dependencies
- Runtime dependencies
- Source code archive for analysis by other tools (e.g. Fossology)

# SPDX: Embedded Focus from the Start

🐙 Born out of a need to exchange OSS component and license information - components and dependencies are the underpinning!

🎂 Recently celebrated its 10<sup>th</sup> birthday - 10 years of use cases produced rich set of dependency relationships.

🎉 SPDX 2.2 became ISO standard in 2021 (ISO/IEC 5962:2021)

Open weekly working group and monthly general meetings.  
Contributors welcome!

## SPDX Supporters

anchore

Bitergia

CANVASS LABS

EMERIN GUARD

CISCO

dynatrace

ECLIPSE FOUNDATION

FOSSA

FOUNDRESIO

Google

GUIDE-RAILS

here

HITACHI Inspire the Next

intel.

Microsoft

MITRE

nexB

paloalto

SCANIA

SIEMENS

snyc

SOURCE Auditor

synopsys

TEXAS INSTRUMENTS

TIDELIFT

TNG TECHNOLOGY CONSULTING

vmware

WNDVR

wipro

XILINX

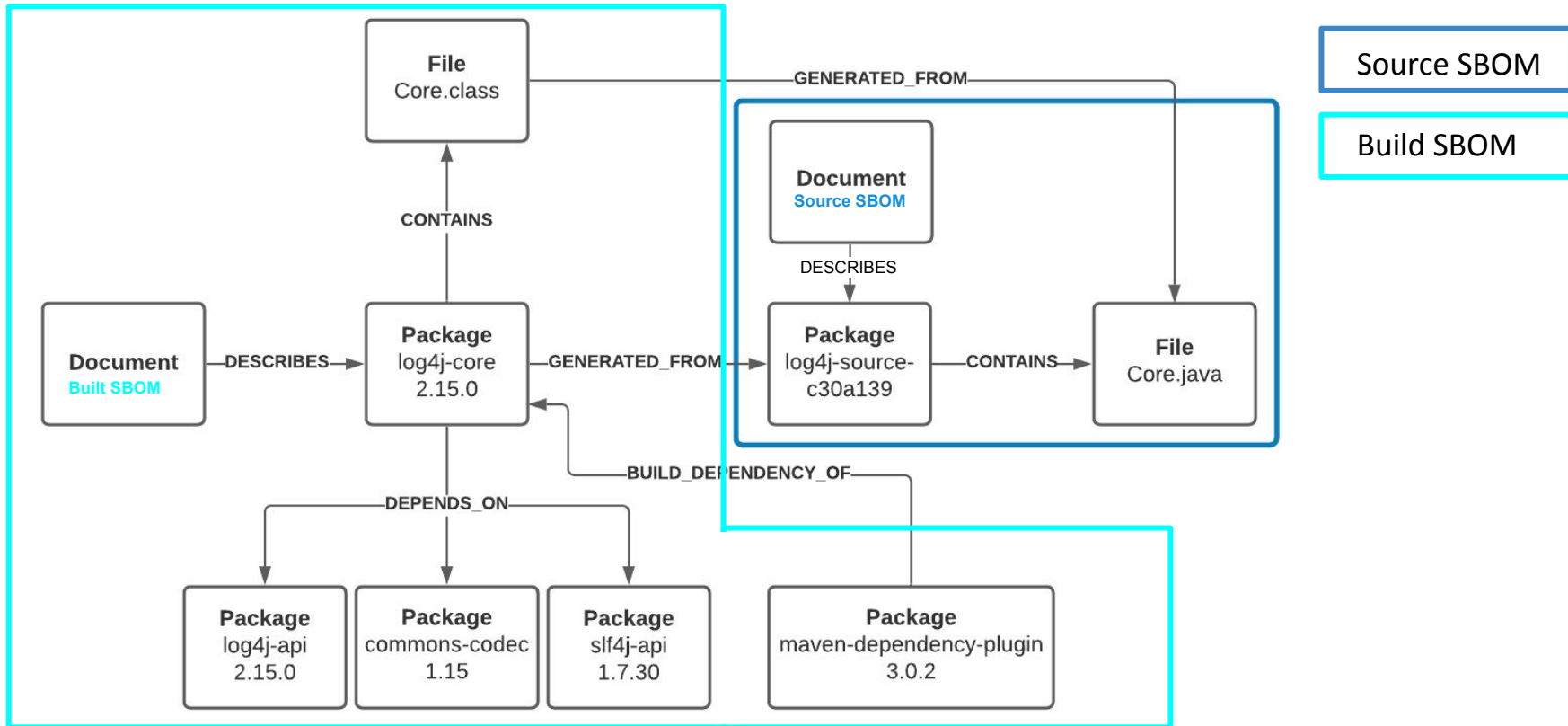
LINUX FOUNDATION

# SPDX Relationships Connect Dependencies Between Components and Between SBOMs

DESCRIBES	DEPENDENCY_OF	PREREQUISITE_FOR	GENERATES	VARIANT_OF
DESCRIBED_BY	RUNTIME_DEPENDENCY_OF	HAS_PREREQUISITE	TEST_OF	FILE_ADDED
CONTAINS	BUILD_DEPENDENCY_OF	ANCESTOR_OF	TEST_TOOL_OF	FILE_DELETED
CONTAINED_BY	DEV_DEPENDENCY_OF	DESCENDENT_OF	TEST_CASE_OF	FILE_MODIFIED
DYNAMIC_LINK	OPTIONAL_DEPENDENCY_OF	DOCUMENTATION_OF	EXAMPLE_OF	PATCH_FOR
STATIC_LINK	PROVIDED_DEPENDENCY_OF	BUILD_TOOL_OF	METAFILE_OF	PATCH_APPLIED
AMENDS	TEST_DEPENDENCY_OF	EXPANDED_FROM_ARCHIVE	PACKAGE_OF	OTHER
COPY_OF	OPTIONAL_COMPONENT_OF	DISTRIBUTION_ARTIFACT	DATA_FILE_OF	
DEPENDS_ON	DEPENDENCY_MANIFEST_OF	GENERATED_FROM	DEV_TOOL_OF	

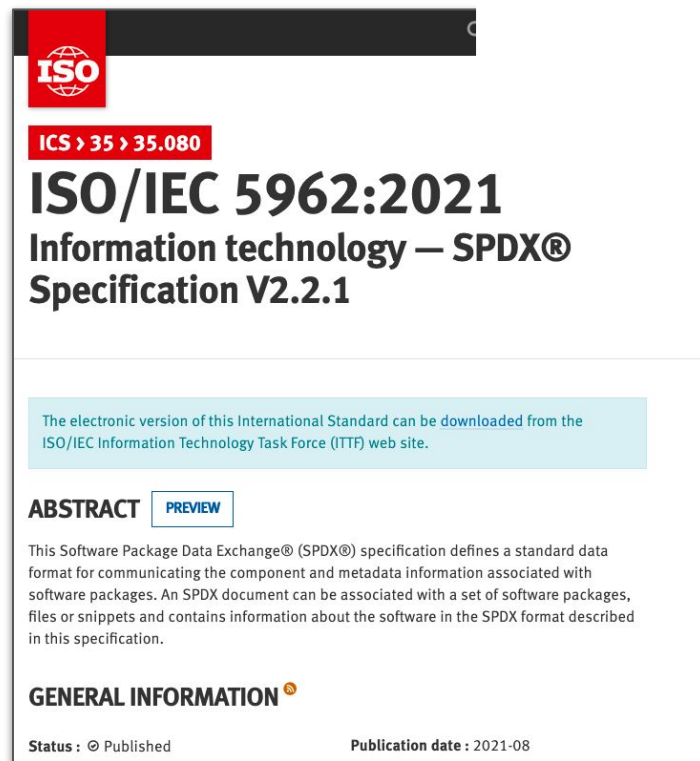
For more details see : <https://spdx.github.io/spdx-spec/relationships-between-SPDX-elements/>

License: CC-BY-4.0



# ISO/IEC 5962:2021

- SPDX is became an ISO/IEC standard in 2021!
- Specification is freely available from [ITTF site](https://www.iso.org/standard/81870.html)
- Future updates are live tracked at: <https://spdx.github.io/spdx-spec>
- For more information on participating in next revisions see <https://spdx.dev/>



The cover page of the ISO/IEC 5962:2021 standard. It features the ISO logo at the top left, followed by the ICS number 35.080. The title 'ISO/IEC 5962:2021 Information technology — SPDX® Specification V2.2.1' is prominently displayed. A light blue box contains a note about downloading the electronic version from the ITTF web site. Below this, there is an 'ABSTRACT' section with a 'PREVIEW' button, followed by a paragraph describing the standard. The 'GENERAL INFORMATION' section at the bottom indicates the status as 'Published' and the publication date as '2021-08'.

**ISO**

ICS > 35 > 35.080

**ISO/IEC 5962:2021**  
**Information technology — SPDX®**  
**Specification V2.2.1**

The electronic version of this International Standard can be downloaded from the ISO/IEC Information Technology Task Force (ITTF) web site.

**ABSTRACT** **PREVIEW**

This Software Package Data Exchange® (SPDX®) specification defines a standard data format for communicating the component and metadata information associated with software packages. An SPDX document can be associated with a set of software packages, files or snippets and contains information about the software in the SPDX format described in this specification.

**GENERAL INFORMATION**

Status : © Published Publication date : 2021-08

Source: <https://www.iso.org/standard/81870.html>  
accessed on 2021/11/19

## I.1 Differences between V2.3 and V2.2.2

V2.3 has added new fields to improve the ability to capture security related information and to improve interoperability with other SBOM formats.

Key changes include:

- Added fields to Clause 7 ( Package Information ) to describe "Primary Package Purpose" and standardize recording of "Built Date", "Release Date", "Valid Until Date".
- Added hash algorithms (SHA3-256, SHA3-384, SHA3-512, BLAKE2b-256, BLAKE2b-384, BLAKE2b-512, BLAKE3, ADLER32 ) to the set recognized by 7.10 (Package Checksum field) and 8.4 (File checksum field)
- Update Clause 7, 8, and 9 to make several of the licensing properties optional rather than requiring the use of "NOASSERTION" when no value is provided.
- Update Clause 11 to add the new relationship types: REQUIREMENT\_DESCRIPTION\_FOR and SPECIFICATION\_FOR.
- Update Annex B ( License matching guidelines and templates ) to use the License List XML format
- Update Annex F ( External Repository Identifiers ) to expand security references to include advisory, fix, URL, SWID. Expand persistent identifiers to include gitoid.
- Update Annex G ( SPDX Lite Profile ) to include NTIA SBOM mandatory minimum fields as required.
- Update Annex H to documented how the snippet information in files to be consistent with REUSE recommendations.
- Added Annex K ( How To Use SPDX in Different Scenarios ) to illustrate linking to external security information, and illustrate how the NTIA SBOM mandatory minimum elements map to SPDX fields.

# To Learn More:

## Software Bill of Materials (SBOM) Guidance:

- <https://www.ntia.gov/SBOM>
- <https://www.cisa.gov/sbom>

## Zephyr SBOM generation:

- Documentation: [Generate Software Bill of Materials with West](#)
- Presentation: [Generating SBOMs for IoT at Build Time](#)
- Presentation: [Zephyr Developer Summit](#) see: <https://sched.co/10CF4>

## Yocto SBOM generation:

- Documentation: [create-spdx in Release 3.4 \(honister\)](#)
- Presentation: [Software Supply Chain with the Yocto Project](#)
- Presentation: [SPDX in the Yocto Project](#)

## SPDX:

- <https://spdx.dev/>
- Documentation: <https://spdx.github.io/spdx-spec/v2.3>





# EMBEDDED LINUX CONFERENCE



OPEN SOURCE SUMMIT  
EUROPE

THE LINUX FOUNDATION

